

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭61-81043

⑬ Int. Cl.⁴

H 04 L 9/00

識別記号

庁内整理番号

Z-7240-5K

⑭ 公開 昭和61年(1986)4月24日

審査請求 未請求 発明の数 1 (全3頁)

⑮ 発明の名称 バケット通信における暗号処理方式

⑯ 特 願 昭59-203110

⑰ 出 願 昭59(1984)9月28日

⑱ 発 明 者	東 充 宏	川崎市中原区上小田中1015番地	富士通株式会社内
⑲ 発 明 者	小 笠 原 弘 二	川崎市中原区上小田中1015番地	富士通株式会社内
⑳ 発 明 者	秋 山 良 太	川崎市中原区上小田中1015番地	富士通株式会社内
㉑ 出 願 人	富士通株式会社	川崎市中原区上小田中1015番地	
㉒ 代 理 人	弁理士 松岡 宏四郎		

明 細 書

1. 発明の名称

バケット通信における暗号処理方式

2. 特許請求の範囲

収容バケット端末装置間を交換接続するバケット交換網において、送信側のバケット端末装置は送信バケット内に含まれるデータを暗号化し、復号化に必要な情報を付加して前記バケット交換網に送出し、受信側のバケット端末装置は該バケット交換網から到着する受信バケットの送信元端末装置を識別し、該受信バケットに含まれる前記復号化に必要な情報に基づき暗号化データを復号化することを特徴とするバケット通信における暗号処理方式。

3. 発明の詳細な説明

(産業上の利用分野)

本発明はバケット交換網を経由して伝達されるデータを暗号化可能とするバケット通信における暗号処理方式に関する。

近年データ通信の発展に伴い、伝送されるデー

タの機密保護が重要視されつつある。

(従来の技術)

第3図は従来ある暗号処理方式の一例を示す図である。

第3図においては、端末装置1および2が伝送路3を介して固定的に接続されている。かかる状態で、端末装置1から端末装置2に伝達するデータを暗号化する為には、端末装置1と伝送路3との間に暗号装置4を挿入し、また端末装置2と伝送路3との間に復号装置5を挿入し、更に暗号装置4で暗号化に使用する鍵および初期値を予め復号装置5に通知して置く。かかる状態で、端末装置1が送出するデータは暗号装置4により所定の鍵および初期値により暗号化され、伝送路3に送出される。該暗号化されたデータは、伝送路3を経由して復号装置5に伝達される。復号装置5は、伝送路3から到着する暗号化されたデータを、暗号装置4と同一の鍵および初期値を用いて復号化し、端末装置2に伝達する。その結果端末装置2は、端末装置1が送信した通りのデータを受信

BEST AVAILABLE COPY

することが出来る。

(発明が解決しようとする問題点)

以上の説明から明らかな如く、従来ある暗号処理方式においては、送信側の端末装置1と受信側の端末装置2とは伝送路3により固定的に接続されていた。その結果復号装置5が復号化に必要な鍵および初期値は、暗号装置4が暗号化に使用する鍵および初期値と常に一致させることが可能であった。

然し端末装置1および2が伝送路3の代わりにパケット交換網を経由して交換接続される場合には、端末装置1からパケット交換網に伝達すべき交換制御情報をも含めて暗号化することは不可能であり、また端末装置2はパケット交換網に收容される端末装置1以外の端末装置からのパケットも受信する為、パケット交換網から伝達される総てのデータを復号装置5により復号化することも不可能となる。

(問題点を解決するための手段)

前記問題点は、收容パケット端末装置間を交換

装置に伝達する。受信側のパケット端末装置においては、送信側のパケット端末装置を識別すると共に受信した前記復号化に必要な情報に基づき暗号化されたデータを復号化する。その結果パケット交換網を経由して伝達されるパケット内のデータは暗号化することが可能となり、機密保護が可能となる。

(実施例)

以下、本発明の一実施例を図面により説明する。第1図は本発明の一実施例によるパケット通信における暗号処理方式を示す図であり、第2図は第1図におけるパケット形式の一例を示す図である。

第1図においては、パケット端末装置7および8がパケット交換網6に收容されている。

今パケット端末装置7が、パケット交換網6を介してパケット端末装置8にデータを暗号化して伝達することを希望し、暗号部71にデータを伝達する。暗号部71は、鍵記憶部72内に設けられている鍵テーブル721から鍵識別符号KIDおよび初期値IVと共に組立部73に伝達する。組立部73は、暗号部71から伝達された発信者識別符号UID、鍵識別符号KID、初期値IVおよび暗号化データEDにデータ長DLを付加してパケットのデータ部を構成し、フラグシーケンスF、アドレスフィールドA、制御フィールドCおよびフレームチェックシーケンスFCSを付加して第2図に示す如き形式のパケットを構成し、パケット交換網6に送出する。

接続するパケット交換網において、送信側のパケット端末装置は送信パケット内に含まれるデータを暗号化し、復号化に必要な情報を付加して前記パケット交換網に送出し、受信側のパケット端末装置は該パケット交換網から到着する受信パケットの送信元端末装置を識別し、該受信パケットに含まれる前記復号化に必要な情報に基づき暗号化データを復号化することとを特徴とする本発明により解決される。

(作用)

即ち本発明によれば、送信側のパケット端末装置はパケット交換網に送出するパケットの内、受信側のパケット端末装置に伝達すべきデータのみを暗号化し、暗号化されたデータを受信側で復号化するに必要な情報、例えば暗号化に使用した鍵或いは初期値を示す諸情報を付加し、パケット交換網が交換制御に必要な情報は暗号化すること無くパケット交換網に送出する。パケット交換網は暗号化されぬ交換制御情報に基づき暗号化されたデータおよび暗号化情報を受信側のパケット端末

て伝達されたデータを暗号化して暗号化データEDを作成し、自端末装置7を識別する発信者識別符号UID、暗号化に使用した鍵を鍵テーブル721から抽出するに用いた鍵識別符号KIDおよび初期値IVと共に組立部73に伝達する。組立部73は、暗号部71から伝達された発信者識別符号UID、鍵識別符号KID、初期値IVおよび暗号化データEDにデータ長DLを付加してパケットのデータ部を構成し、フラグシーケンスF、アドレスフィールドA、制御フィールドCおよびフレームチェックシーケンスFCSを付加して第2図に示す如き形式のパケットを構成し、パケット交換網6に送出する。

パケット交換網6は、パケット端末装置7から伝達されたパケットのアドレスフィールドAおよび制御フィールドCを分析し、宛先のパケット端末装置8に送達する。

パケット端末装置8においては、分解部81がパケット交換網6から到着するパケットを分解し、データ部に含まれる発信者識別符号UIDおよび

BEST AVAILABLE COPY

鍵識別符号 K I D を抽出し、鍵記憶部 8 2 に伝達すると共に、初期値 I V および暗号化データ E D を復号部 8 3 に伝達する。鍵記憶部 8 2 は、各送信側バケット端末装置 7 等が鍵記憶部 7 2 等に保有すると同一の鍵テーブル 8 2 1 乃至 8 2 n を具備しており、分解部 8 1 から伝達された発信者識別符号 U I D に対応する鍵テーブル（例えば 8 2 1）を求め、該鍵テーブル 8 2 1 から鍵識別符号 K I D に基づき送信側バケット端末装置 7 が鍵テーブル 7 2 1 から抽出したと同一の鍵を抽出し、復号部 8 3 に伝達する。復号部 8 3 は、鍵記憶部 8 2 から伝達された鍵および分解部 8 1 から伝達された初期値 I V を用いて、分解部 8 1 から伝達された暗号化データ E D を復号化し、送信側バケット端末装置 7 が暗号部 7 1 に入力したと同一のデータを得る。

以上の説明から明らかな如く、本実施例によれば、バケット端末装置 7 からバケット端末装置 8 には暗号化データ E D が発信者識別符号 U I D、鍵識別符号 K I D および初期値 I V と共に伝達さ

れ、受信側バケット端末装置 8 は暗号化データ E D を復号化可能となる。なおバケット交換網 6 がバケットをバケット端末装置 8 に伝達するに必要なアドレスフィールド A 或いは制御フィールド C に含まれる交換制御情報は暗号化されることなくバケット端末装置 7 から送出される為、バケット交換網 6 は該バケットを確実にバケット端末装置 8 に送達可能となる。

なお、第 1 図および第 2 図はあく迄本発明の一実施例に過ぎず、例えばバケット端末装置 7 および 8 の構成は図示されるものに限定されることは無く、他に幾多の変形が考慮されるが、何れの場合にも本発明の効果は変わらない。また第 1 図において使用されるバケット形式は図示されるものに限定されることは無く、他に幾多の変形が考慮されるが、何れの場合にも本発明の効果は変わらない。

〔発明の効果〕

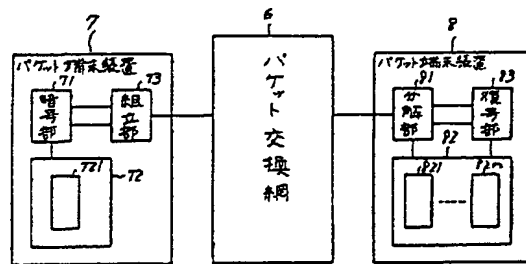
以上、本発明によれば、前記バケット交換網において、収容バケット端末装置間で任意に暗号化

データが伝達可能となり、当該バケット交換網の機密保護性が向上する。

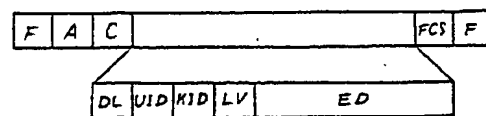
4. 図面の簡単な説明

第 1 図は本発明の一実施例によるバケット通信における暗号処理方式を示す図、第 2 図は第 1 図におけるバケット形式の一例を示す図、第 3 図は従来ある暗号処理方式の一例を示す図である。

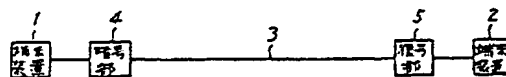
図において、1 および 2 は端末装置、3 は伝送路、4 は暗号装置、5 は復号装置、6 はバケット交換網、7 および 8 はバケット端末装置、7 1 は暗号部、7 2 および 8 2 は鍵記憶部、7 3 は組立部、8 1 は分解部、8 3 は復号部、7 2 1 および 8 2 1 乃至 8 2 n は鍵テーブル、A はアドレスフィールド、C は制御フィールド、DL はデータ長、ED は暗号化データ、F はフラグシーケンス、FCS はフレームチェックシーケンス、I V は初期値、K I D は鍵識別符号、U I D は発信者識別符号、を示す。



第 1 図



第 2 図



第 3 図

代理人 弁理士 松岡宏四郎

